# مروري بر رفتارشناسي هكرها در دنياي سايبر

نويسنده: امير حسين شريفي( Amirsh@sgnec.net )

**شهرت و اعتبار گذشته**


در گذشته اخبار بسيار زيادي درباره هك شدن سايت هاي مختلف شنيده مي شد كه در آن يك مهاجم با استفاده از روش هاي بعضاً ابتدايي صفحه اول يك سايت را دستكاري مي كرد. هدف عمده اين دسته از مهاجمان شهرت و اعتبار بود كه از اين طريق در صدد جذب آن بودند.

در آن زمان يكي از اموري كه باعث مي شد اينگونه هكرها در كار خود جدي تر شوند اطلاع رساني سايت هاي خبري درباره آنها بود و همين موضوع باعث برافروخته تر شدن آتش شهرت طلبي آنها مي گشت و آنها را در اهداف خود جدي تر مي كرد.

**همين حالا شروع كنيد!**

بعد از گذشت يك دوره تقريباً دو ساله خواسته هاي مهاجمان تغيير كرد و خواسته هاي شهرت طلبي به خواسته هاي اقتصادي و بعضاً سياسي تبديل شد. يكي از تبعات اين رويكرد باز شدن سايت هاي خريد و فروش اكسپلويت ها بود. هدف اين دسته از سايت هاي خريد و فروش حفره هاي پيدا شده توسط محققان امنيتي است. شايد باوركردني نباشد كه ارقامي كه براي هر كد اكسپلويت پرداخت مي شود تا ۲۰۰۰۰ دلار نيز بوده است. هر چند در دنياي زيرزميني هكرها ارقام پيشنهادي بالاتر نيز پيدا خواهيد كرد.

كافي است در زمينه فروش كدهاي مخرب يك سوال ساده از دكتر گوگل بپرسيد تا لينك هاي فراواني از سايت هاي معروف و غير معروف و بعضاً زير زميني براي شما به نمايش بگذارد.

بسيار خب، برنامه نويس هاي حرفه اي مي توانند از همين الان كار خود را شروع كنند، البته قبل از شروع بايد يك سري تخصص هاي مربوط به اين تجارت را داشته باشيد و تمرينات زيادي انجام دهيد. اما بعد از اين سختي ها شما هم مي توانيد در بازار خريد و فروش كدهاي مخرب (اكپسلويت ها) وارد شويد و شانس خود را

آزمايش كنيد و در كنار كار اصلي خود به سرگرمي آناليز نرم افزارها بپردازيد و پول هاي هنگفتي را از اين طريق به جيب بزنيد.

با پيشنهاد اين مبالغ هنگفت بسياري از كارشناسان و محققان امنيتي به سمت اينگونه تحقيقات گسيل شدند و هنوز هم اين تجارت به قوت خود باقيست و همه مي توانند در آن شركت كنند.

**هرزنامه ها؛ خانمان برانداز اما پردرآمد!**

اما دنياي هكرهاي بداندیش به گونه اي ديگر رقم خورد. آنها از كدهاي خود در صدد تجهيز شبكه هاي Bot بر آمدند. حتما مي دانيد كه شبكه هاي Bot لشگري از قرباني هايي هستند كه به آنها زامبي گفته مي شود. خود كلمه زامبي معناي جالبي دارد. زامبي به بدني گفته مي شود كه يك روح ديگر در آن رسوخ كرده است و آن را تحت كنترل خود در آورده است.

كامپيوترهاي زامبي نيز به سيستم هايي گفته مي شود كه توسط رييس خود و به صورت متمركز كنترل مي شود. در گذشته از زامبي ها فقط در جهت حملات DDoS استفاده مي شد اما امروزه روش كاري فرق كرده است و هكرها ترجيح مي دهند از لشگر زامبي هاي خود درآمد كسب كنند! حتما مي پرسيد چگونه؟

امروزه هرزنامه ها براي تمامي شبكه ها معضل بزرگي شده اند. دريافت روزانه ده ها هزار هرزنامه باعث شده است كه مديران شبكه در صدد صرف هزينه هاي زيادي براي خلاصي از آنها برآيند. بررسي ها نشان مي دهد كه بيش از نيمي از پهناي باند يك سرور ايميل صرف پردازش هرزنامه ها مي گردد. اگر بخواهيم اين هزينه را در ايران بررسي كنيم شايد بتوان گفت شركتهاي متوسط به بالا به طور سالانه بيش از ۵ ميليون تومان هزينه دريافت هرزنامه مي پردازند و اين فقط ضرر مالي حاصل از اشغال بيهوده پهناي باند است.

اما تا به حال از خودتان پرسيده ايد كه چه آدم هاي بيكاري با چه روشي اين همه ايميل ارسال مي كند؟ در گذشته اين كار توسط برخي برنامه هاي ارسال هرزنامه و به صورت متمركز انجام مي شد كه نياز به يك پهناي باند زياد جهت ارسال هرزنامه ها داشت. هرچند هكر ها اين پهناي باند را از طريق برخي سرورهاي هك شده تامين مي كردند اما اين سرور ها به سرعت شناسايي مي شدند و در ليست سياه ضد هرزنامه ها قرار مي گرفتند.

اما هكر ها هميشه راههاي جديدي را پيدا مي كنند كه نشان دهنده نبوغ فكري آنهاست. امروزه هكرها فقط با چند دستور ساده ده ها هزار هرزنامه را در كمتر از چند دقيقه ارسال مي كنند! تعجب نكنيد زيرا اين بار لشگري از زامبي ها نيز آنها را براي رسيدن به اين هدف كمك مي كنند.

همه چيز به صورت خودكار براي آنها فراهم است. روش كار بسيار ساده است اما مقابله با آن بسيار سخت و ناممكن!

شناسايي اينگونه هرزنامه ها براي برنامه هاي ضد هرزنامه مشكل و ناممكن است زيرا كه اين بار ايميل ها از سمت اشخاص حقيقي (زامبي ها) ارسال مي گردد و همه چيز طبيعي و واضح است!

كرمهاي آنها كه به صورت موروثي رشد مي كنند و تمام خصوصيات پدران خود را به ارث مي برند قوي تر از روزهاي قبل، در خدمت رييس، شبكه Bot را گسترش مي دهند و روحهاي بيشتري را تسخير مي كنند. رييس فقط پشت سيستم خود و يا هر سيستم ديگر به شبكه (احتمالا IRC ) متصل مي شود و دستورات لازم را براي سربازان خود ارسال مي كند. آنها نيز بدون چون و چرا گوش به فرمان رييس هستند.

همه چيز براي كسب درآمد چند ميليون دلاري مهياست. فقط كافي است سفارش هاي بيشماري را جهت ارسال هرزنامه بگيرند و فقط با چند دستور ساده پولهاي هنگفتي را به جيب بزنند!

**وب سايت هاي آلوده، معضل جدي**

بد نيست كمي هم به روش هاي جديد نفوذ به سيستم ها و بزرگ كردن شبكه هاي Bot بپردازيم.

راههاي سنتي روش هاي نفوذ به سيستم ها و بزرگ كردن شبكه هاي Bot، ايجاد كرم هاي اينترنتي مختلف و موروثي مي باشد كه در بالا بخشي از آن ذكر شد.

اما هكر ها اين بار نيز روش هاي جديدي را به كار برده اند.

در گذشته وقتي يك سايت اينترنتي تحت كنترل يك هكر قرار مي گرفت، با تغيير صفحه اول سايت و فقط جهت كسب شهرت آن را در بوق و كرنا مي كرد كه اين سايت توسط گروه و يا شخص من هك شد. هر چند هنوز اين فرهنگ در ايران پا برجاست اما در دنياي حرفه اي سايبر، با تغيير اهداف هكر ها اينگونه روش ها نيز منسوخ شده است و آنها ترجيح مي دهند از بازديد كنندگان اين سايت ها در جهت اهداف اقتصادي خود بهرمند شوند!

امروزه عمده كاربران براي جستو و مرور اينترنت از دو مرورگر IE متعلق به مايكروسافت و Firefox متعلق به موزيلا، استفاده مي كنند. از اين رو تير تحقيقات هكر ها جهت يافتن حفره هاي امنيتي به سمت اين دو مرورگر شليك شده است. به گونه اي كه ابزارهاي خودكار زيادي براي يافتن كدهاي مخرب در اين دو مرورگر منتشر شده است و پديده هايي همچون "يك ماه حفره در مرورگر... " به وجود آمدند.

بسيار خب، همه چير مهياست براي نفوذ و تجهيز شبكه هاي Bot با لشگري از سيستم هاي آسيب پذير بي گناه! كافي است ابتدا يك سايت (يا يك سرور ميزبان) تحت كنترل يك مهاجم قرار گيرد. هكر، كدهاي مخرب خود را كه اغلب ناشناس و به اصطلاح 0-day است را به طور گسترده در لابه لاي سايت هاي اصلي اضافه مي كند. كدهاي مخرب بي سرو صدا و بدون هيچ پيغام خاصي روي سيستم هاي بازديدكنندگان نصب مي شوند و فاجعه اي را شروع مي كنند.

كم كم وب سايت هاي آلوده در حال تبديل شدن به يك معضل بزرگ براي مديران شبكه ها و كاربران است. اين مشكل آنقدر حاد است كه محققان امنيتي اعتراف كردند كه اينگونه حملات از پوشش رادارهاي امنيتي آنها خارج شده اند و كنترل آنها در بعضي مواقع ناممكن است.

بنا بر تحقيقات برخي شركت هاي امنيتي، بيش از ۵۰ درصد كدهاي مخربي كه توسط هكرها در اين سايت ها استفاده مي شوند ناشناس است و آنتي ويروس ها توانايي شناسايي آنها را ندارند و اين يعني فاجعه!!

ابعاد اين فاجعه زماني بزرگ تر مي شود كه سايت هاي جستجو نيز به كمك هكر ها بيايند و كدهاي مخرب آنها را در پشت سرور هاي خود پنهان كنند. بنا بر تحقيقاتي كه توسط يك شركت امنيتي صورت گرفته است نشان مي دهد هفته ها و ماهها طول مي كشد تا سايت ها و صفحات آلوده اي كه در موتورهاي جستجو ذخيره شده اند با نسخه هاي پاك و غير الوده جايگزين شوند. اين مشكلي است كه در سال گذشته شركت فينجان نيز به آن اشاره كرده بود و اسم آن را cache Poisoning گذاشته بود.

**جنگ سرد دولت ها روي تارهاي عنكبوت**

اما دنياي سايبر فقط به هكرهايي ختم نمي شود كه اهداف اقتصادي را دنبال مي كنند. اجازه بدهيد سري هم به دنياي سياست بزنيم. جايي كه ميليون ها دلار صرف مي شود تا اطلاعات مختصري از دشمن جمع آوريگردد!

در خبرهاي چند ماه قبل خوانديم كه چگونه هكرهاي چيني سيستم هاي پنتاگون را مورد حمله قرار دادند و اطلاعات محرمانه اي را به سرقت بردند. چند هفته بعد نيز برخي سيستم هاي دولت بريتانيا نيز مورد نفوذ قرار گرفت اين بار هم چيني ها در اين نفوذ دست داشتند. هر چند دولت چين دخالت خود را در اين حملات به شدت انكار كرده است اما وقتي اين حمله به سيستم هاي بانكي و دولتي كشور آلمان در زمان ملاقات مركل و جيانگ زمين نيز سرايت كرد همگان باور كردند كه جرياني در راه است!

شايد هكرهاي چيني اولين كسي نباشند كه قصد نفوذ به

سيستم هاي دولتي رقباي خود را داشته باشند. دولت ايالات متحده و دولت بريتانيا هر كدام به صورت رسمي نيز اعلان كرده اند سايتهايي را جهت انجام امور جاسوسي از كشورهاي ديگر ايجاد كرده اند. اين سايتها در زمينه جاسوسي از طريق دنياي سايبر فعاليت مي كنند.

با اين روالي كه كشورهاي قدرتمند دنيا در پيش گرفته اند حتما در سال آينده شاهد جنگي سرد در پهنه كابلهاي مسي و فيبر هاي نوري خواهيم بود. جنگي كه امروز از آزمايشگاههاي حساس وزارت دفاع امريكا شروع شده است، اما پايان آن نامشخص است!

در اين ميان ما در كجا قرار داريم؟ اين سوالي است كه همه بايد به آن فكر كنيم.